Chapter 5: Using your CRYPTOCard

Strengthened machines are configured to respond in *portal mode* when requests for access come from unKerberized machines. In portal mode the strengthened machine acts as a secure gateway into the strengthened realm, requiring a single-use password for authentication. A CRYPTOCard is a calculator-style, battery-powered device used for generating a single-use password.

To obtain a CRYPTOCard, go to the *Request Form for Computing Username and Primary Accounts* at `http://computing.fnal.gov/cd/forms/acctreq_form.html`.

☞ As of March 2002, new CRYPTOCards operate a little differently from those previously sent from the vendor. When you get your CRYPTOCard, first carefully read the instruction card that comes with it.

5.1 How does your CRYPTOCard Work?

Before we issue you your CRYPTOCard, we initialize it and synchronize it with the Kerberos Key Distribution Center[1] (KDC). This process (a) associates the card with your principal, (b) sets an initial PIN on the card, and (c) creates a secret encryption key stored in both the KDC and the card.

1. The KDC is the "keymaster" of the Kerberos authentication service for all the machines in the realm. It runs on a server maintained by Fermilab's computing security team. Every principal and every initialized CRYPTOCard shares a unique encryption key with the KDC, allowing the KDC to verify the identity of each user/service request.

The KDC and the CRYPTOCard operate independently on the identical strings using the shared key, and they produce the same result. Roughly half of this resulting string is to be used as the first one-time password, the other half (plus/minus some overlapping bits) is stored for later use as the next string on which both parties will operate. And so on.

The string on which the shared key operates is called the *challenge*. The portion of the result used as the password is called the *response*. The first challenge is chosen by the KDC when you use the card.

5.2 Caring for your CRYPTOCard

You will find printed instructions with your new CRYPTOCard. Carefully read *Use and Care of your RB-1 Authentication Token*, and *Battery Replacement*.

Here we highlight a few points that we think are important:

- Your CRYPTOCard is relatively expensive; please don't lose it! Treat it as you would your house keys (if they were breakable!).
- Your CRYPTOCard looks the same as your colleague's, so make a note of the serial number printed on the back so that you can identify yours. Even though another person would need both your principal and your PIN to use your card, we recommend that you don't label your card with anything that resembles your principal. In most cases this means don't put your name on it. You can label it with a non-identifying word or sticker that you'll recognize.
- Don't drop, sit on or crush the card (don't carry it in your back pocket).
- Keep it dry and out of intense heat or cold. Don't let it go through the laundry, and don't leave it in your car in the winter or summer.
- When the display becomes dim, it's time to replace the batteries (two new CR2016, 3V lithium coin cells). CHANGE THEM ONE AT A TIME TO PREVENT DATA LOSS! Otherwise you will need to get the card reprogrammed.

5.3 Usage Notes

- We recommend using fingertips or a pencil eraser for pressing the CRYPTOCard buttons. Fingernails, pen tips and other sharp objects work less well. You don't need to remove it from the plastic cover to use it.

- When you first turn on the card, it takes a second or two to respond with a prompt.
- If you ever forget your PIN (see section 5.4) or if the card locks up (says "locked" when turned on), send email to `compdiv@fnal.gov` to arrange getting your CRYPTOCard reprogrammed. If you are on-site, you will need to come to WH8NE. If you are off-site, mention that in your email.
- Your CRYPTOCard will automatically turn itself off after 60 seconds unless it receives further input.

5.4 The First Thing to do: Reset your PIN

The CRYPTOCard comes with an initial PIN (personal code to prevent use by other individuals) that you are required to reset. The minimum length of the PIN is four digits, but it can be as long as eight. When entering your PIN, you are limited to seven consecutive wrong tries before lockout.

5.4.1 Resetting Initial PIN

Original Style Card

1) Press the **ON/OFF** button to turn on the card, enter your initial PIN and press **ENT**.

2) At the prompt `New PIN?` enter a new PIN and press **ENT**.

3) At the `Verify` prompt, enter your new PIN again and press **ENT**. The card displays a preconfigured string which you can ignore.

4) If you're not going to log on now, you can turn off the card or let it do so automatically.

New Style Card (March 2002)

1) Press **CHG PIN** (actually any of the 4 keys **PASSWORD**, **DIG SIG**, **MENU** and **CHG PIN** will work).

2) At the prompt: `PIN?` enter your initial PIN.

3) At the prompt: `New PIN?` enter a new PIN and press **ENT**.

4) At the `Verify` prompt, enter your new PIN again and press **ENT**. It displays: `Card OK`

5) If you're not going to log on now, you can turn off the card or let it do so

automatically.

5.4.2 Resetting PIN (General)

Original Style Card

For subsequent PIN changes, turn the card on and enter your PIN followed by **ENT**. At the `Fermilab` prompt, press **CPIN** and proceed from step (2) for this style card, above.

New Style Card (March 2002)

For subsequent PIN changes, turn the card on using the CHG PIN button, and enter your (old) PIN followed by **ENT**. At the `New PIN?` prompt proceed from step (3) for this style card, above.

5.5 Log in Using CRYPTOCard (the First Time)

5.5.1 Original Style Card

1) Turn on your CRYPTOCard and enter your new PIN, followed by **ENT**.

2) The card is configured to display the id `Fermilab`. Press **ENT** when you see it. You'll see a preconfigured *challenge*, which you can ignore.

3) Run **ssh**, **slogin**, **telnet**, or **ftp** normally on your nonKerberized machine to the strengthened host, and enter your login id at the host prompt. The first time you use the card, the host system (in portal mode) displays the message:

```
Press CH/MAC and enter this on the keypad: [12345678]
Enter the displayed response:
```

where `12345678` is a sample eight-digit *challenge*.

4) On your CRYPTOCard, press **CH/MAC**, then type the *challenge* displayed on the host system into your CRYPTOCard. If you mistype, press **CLR** and re-enter the *challenge*. Press **ENT** to get a *response* of eight hex digits.

5) Enter the CRYPTOCard *response* at the host system prompt (it is not case-sensitive). Press **RETURN**, and you should be logged in with

Kerberos tickets.

6) Turn off your CRYPTOCard, or let it do so automatically.

5.5.2 New Style Card (March 2002)

Before the initial login, you need to synchronize the card with our KDC.

1) Run **ssh**, **slogin**, **telnet**, or **ftp** normally on your nonKerberized machine to the strengthened host, and enter your login id at the host prompt. The host system (in portal mode) displays an eight-digit *challenge*.

2) Press **MENU** to turn on your CRYPTOCard, and enter your PIN as required, followed by **ENT**.‘

3) Ignore the `Adj LCD` or `Contrast` prompt (the latter appears on cards issued after November 2002) and press **MENU** again.

4) At the prompt `ReSync`, press **ENT**.

5) At the prompt `Ready` (for cards issued Nov. ‘02 or later, you see a flashing cursor instead), key the challenge displayed on your monitor into your CRYPTOCard, and press **ENT** to get a *response* of eight hex digits. (If you mistype, press **CLR** and re-enter the *challenge*. **CLR** clears one character at a time, or it will clear the whole field if held down for more than one second.)

6) The *response* (password) associated with that challenge now displays on the CRYPTOCard.

7) Enter the CRYPTOCard response at the host system prompt (it is not case-sensitive). Press **RETURN**, and you should be logged in with Kerberos tickets.

5.6 Log in Using CRYPTOCard (Subsequently)

5.6.1 Original Style Card

1) Turn on your CRYPTOCard and enter your PIN, followed by **ENT**. (You are limited to seven consecutive wrong-PIN tries before lockout.)

2) The card is configured to display the id `Fermilab`. Press **ENT** when you see it. The CRYPTOCard displays a *challenge*.

3) Run **ssh**, **slogin**, **telnet**, or **ftp** normally on your nonKerberized machine to the strengthened host, and enter your userid at the host prompt. The host system (in portal mode) displays the message:

```
CryptoCard RB-1
Press ENTER and compare this challenge to the one on your
display
Challenge is [12345678], Enter the displayed response:
```

where `12345678` is a sample eight-digit *challenge*.

4) Compare the *challenge* on the host to the one on the CRYPTOCard:

a) If the *challenges* are the same, press **ENT** again on the CRYPTOCard to get the *response*. (In this case the KDC and your CRYPTOCard are synchronized. As long as they remain in sync, the CRYPTOCard will generate the right *response*.)

b) If the *challenges* are different (you may see all zeroes), press **CH/MAC** on the CRYPTOCard and enter the *challenge* displayed on the host system into the card. (This resynchronizes the CRYPTOCard.) Then press **ENT** to get the *response*.

5) Enter the *response* at the host system prompt. Press **RETURN** and you should be logged in with tickets.

6) Turn off your CRYPTOCard, or let it do so automatically.

5.6.2 New Style Card (March 2002)

There are two ways to use the CRYPTOCard to log in, one using the **PASSWORD** key and the other using **DIG SIG**.

PASSWORD

IN THIS MODE, THE CRYPTOCARD DOES NOT DISPLAY THE CHALLENGE!

1) Run **ssh**, **slogin**, **telnet**, or **ftp** normally on your nonKerberized machine to the strengthened host, and enter your userid at the host prompt. The host system (in portal mode) displays the message:

```
Press ENTER and compare this challenge to the one on your
display: [12345678]
Enter the displayed response:
```

where `12345678` is a sample eight-digit *challenge*.

2) Press **PASSWORD** to turn the CRYPTOCard on

3) At the `PIN?` prompt, enter your PIN followed by **ENT**.

4) The card is configured to display the id `Fermilab`. Press **ENT** when you see it.

5) The card now displays the response, not the challenge! If the card is synchronized with the KDC, this response will work. If not, using **DIG SIG** (below) will work, but before ever using **PASSWORD** again, you'll have to resynchronize your card.

6) Enter the response at the host system prompt. Press **RETURN** and you should be logged in with tickets.

DIG SIG

This method works even if your card has gotten out of sync (assuming that initial synchronization has been done), but it does not resynchronize your card for future logins. A drawback to this method is that you have to key the challenge into your CRYPTOCard each time.

1) Run **ssh**, **slogin**, **telnet**, or **ftp** normally on your nonKerberized machine to the strengthened host, and enter your userid at the host prompt. The host system (in portal mode) displays the message:

```
Press ENTER and compare this challenge to the one on your
display: [12345678]
Enter the displayed response:
```

where `12345678` is a sample eight-digit *challenge*.

2) Press **DIG SIG** to turn the CRYPTOCard on

3) At the `PIN?` prompt, enter your PIN followed by **ENT**.

4) At the `Ready` prompt, enter the challenge (displayed on your monitor) into the CRYPTOCard, and press **ENT**. (If you mistype, press **CLR** and re-enter the challenge. **CLR** clears one character at a time, or it will clear the whole field if held down for more than one second.)

5) The card now displays the response.

6) Enter the response at the host system prompt. Press **RETURN** and you should be logged in with tickets.

5.7 Reauthenticate using your CRYPTOCard

To remain logged in and reauthenticate safely, issue the command:

```
% new-portal-ticket
```

This provides a portal mode prompt, and allows you to use your CRYPTOCard as in section 5.6 *Log in Using CRYPTOCard (Subsequently)* to get new tickets. E.g.,:

```
Press ENTER and compare this challenge to the one on your
display: [12345678]
Enter the displayed response: <enter response>
18960 Terminated
Connection closed by foreign host.
```

Don't be dismayed by the messages that appear! The **`new-portal-ticket`** command works by opening a telnet connection to "localhost" and letting the user answer the portal challenge. There's a sleep command going on to keep the telnet connection from closing too soon, and `Terminated` comes when that sleep is no longer needed and is killed by the script. `Connection closed...` comes when that telnet session is over.

5.8 Resync your CRYPTOCard

5.8.1 Original Style Card

Commence the login procedure as outlined in 5.6 *Log in Using CRYPTOCard (Subsequently)*. If the *challenges* are different, press **CH/MAC** on the CRYPTOCard and enter the *challenge* displayed on the host system into the card. (This resynchronizes the CRYPTOCard.) Then press **ENT** to get the *response*.

5.8.2 New Style Card (March 2002)

1) Run **ssh**, **slogin**, **telnet**, or **ftp** normally on your nonKerberized machine to the strengthened host, and enter your login id at the host prompt. The host system (in portal mode) displays an eight-digit *challenge*.

2) Press **MENU** to turn on your CRYPTOCard, and enter your PIN as required, followed by **ENT**.

3) Ignore the `Adj LCD` prompt and press **MENU** again.

4) At the prompt `ReSync`, press **ENT**.

5) At the prompt `Ready`, key the challenge displayed on your monitor into your CRYPTOCard, and press **ENT**. (If you mistype, press **CLR** and re-enter the *challenge*. **CLR** clears one character at a time, or it will clear the whole field if held down for more than one second.)

Your card is now resynchronized and the correct *response* now displays on the CRYPTOCard. You can complete your login at this point by typing the response at the host system prompt, followed by **RETURN**.